Joshua Adam Schulte, *pro se*

September 14, 2021

BY HAND

Judge Paul A. Crotty
United States District Judge
Southern District of New York
500 Pearl Street
New York, New York 10007

RE: *United States v. Joshua Adam Schulte*, S3 17 Cr. 548 (PAC)

Dear Judge Crotty:

I write to notify the Court of a Brady Violation committed by the government. In reviewing last-minute disclosures before the first trial, I noticed references to the CIA's Advanced Forensics Division (AFD) and the WikiLeaks Task Force (WTF) regarding forensic examinations and analysis performed on DevLAN and the alleged crime scene that the government has concealed from the defense to this date. This information only confirms the critical nature of the digital forensics in this case.

Specifically, Agent Evanchec wrote in a Lync message: "Couple things: 1. AFD previously assessed it was not possible that the info Wiki had to have come from a backup. As of Friday, that was walked back. The error they thought was in the backup script was not actually there. As such, there was a backup of the Atlassian products on the FIle Share that every DevLAN user had access to. Bottom line: subject pool is every DevLAN user now. This may be significant in terms of PC for future warrants."

The CIA's forensic division determined that every DevLAN user had access to the leaked CIA information, and that the government's convoluted and confusing theory of prosecution completely unnecessary. This would have been very useful to know before the first trial, specifically the forensic analysis and location of this file share and backup. The government never produced this AFD forensic report, nor did it produce any forensic report from either AFD or the WTF. In light of this outrageous Brady Violation, I want to once again highlight the significance of the defense's dire need for access to the alleged forensic crime scene to mount a defense and subject the government's case to adversarial testing paramount to any fair trial.

I. THE BRADY VIOLATION

"The government has a duty to disclose evidence favorable to the accused when it is material to guilt or punishment." *United States v. Madori*, 419 F.3d 159, 169 (2d Cir. 2005) (citing *Bradley v. Maryland*, 373 US 83, 87 (1963)). To prove a Brady violation, a defendant must establish that (1) the evidence at issue is "favorable to the accused"; (2) the evidence was "suppressed by the state, either willfully or inadvertently"; and (3) "prejudice... ensued" from the lack of disclosure such that it is "material." *Strickler v. Greene*, 527 US 263, 281-82 (1999); *United States v. Coppa*, 267 F.3d 132, 140 (2d Cir. 2001).

As to the first element, evidence that is "favorable to the accused" includes not only evidence that tends to exculpate the accused, but also evidence that is useful to impeach the credibility of a government witness," that is, *Giglio* material. *Coppa*, 267 F.3d at 139 (citing *Giglio v. United States*, 405 US 150, 154 (1972)). Here, the AFD's forensic report is clearly favorable to the accused—it severely undermines the prosecution's case-in-chief. It is especially important because to this date the government has concealed the forensic crime scene to hide other exculpatory evidence from the defense. Additionally, the fact that trained forensic expert CIA officers would testify differently than the government's supposed experts is also incredibly favorable.

As to the second element, a defendant must show that the government suppressed evidence, meaning that the government violated its "affirmative duty to disclose favorable evidence known to it." *United States v. Payne*, 63 F.3d 1200, 1208 (2d Cir. 1995). "[T]he government cannot be required to produce that which it does not control and never possessed or inspected." *United States v. Hucher*, 622 F.2d 1083, 1088 (2d Cir. 1980) (quoting *United States v. Cannifl*, 521 F.2d 565, 573 (2d Cir. 1975)). A prosecutor, however, is "presumed... to have knowledge of all information gathered in connection with his office's investigation of the case and indeed "has a duty to learn of any favorable evidence known to the others acting on the government's behalf in the case, including the police.'" *United States v. Avellino*, 136 F.3d 249, 255 (2d Cir. 1998) (quoting *Kyles v. Whitley*, 514 US 419, 437 (1995)). It is clear that the government possessed the AFD and other forensic reports because the FBI case agent specifically reported the report's findings.

As to prejudice and materiality, a defendant must show that "there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different." *Turner v. United States*, 137 S. Ct. 1885, 1893 (2017) (quoting *Cone v. Bell*, 556 US 449, 469-70 (2009)). "A reasonable probability of a different result is one in which the suppressed evidence undermines confidence in the outcome of the trial." *Id.* (internal quotation marks omitted) (quoting *Kyles*, 514 US at 434); see also *Strickler*, 527 US at 281 ("[T]here is never a real 'Brady Violation' unless the nondisclosure was so serious that there is a reasonable probability that the suppressed evidence would have produced a different verdict."). "Where the evidence against the defendant is ample or overwhelming, the withheld Brady material is less likely to be material than if the evidence of guilt is thin." *United States v. Gil*, 297 F.3d 93, 103 (2d Cir. 2002). The government tried an extremely weak circumstantial case in which the jury was deadlocked. If the defense had access to the AFD's and WTF's forensic analysis, as well as the ability to subpoena the CIA's analysists to testify at trial, then the jury easily would have swung to acquittal. The fact that the government concealed this critical Brady material is unconscionable.

II. PRIOR BRADY VIOLATION

I also note for the Court that the government tried to hide other information from the defense in violation of *Brady*. The defense moved for a mistrial when it was discovered that the government hid information about CIA employee Michael before trial. Specifically, the government failed to disclose an internal August 2019 memorandum from the Deputy Director of the CIA for Counterintelligence to the Director of Security requesting that Michael be placed on enforced administrative leave because of suspicion, *inter alia*, that he was involved in the theft and disclosure of the Vault 7 and Vault 8 information (the "CIA Memorandum"). See Brady Violation letter, dated February 18, 2020 (Dkt. 328) and February 22, 2020 (Dkt. 331).

III. THE FORENSIC CRIME SCENE

This Brady Violation highlights and reinforces the defense's critical need for access to these same forensic materials that the government provided to its own experts to advance its case-in-chief, but concealed from the defense. Without access to the forensic crime scene, the defense cannot advocate any defense. The government can easily hide all the exculpatory forensic evidence, and if ever they are discovered then they can simply claim their experts "missed" that evidence. The government cannot have their cake and eat it too: If they want to allege complex computer crimes against the CIA then they must turn over these computers; it is a manifest injustice to deny the defense the ability to mount a complete defense.

A. History of requests for access to the forensic crime scene

1. Initial Requests

The defense first requested the government produce the forensic crime scene in discovery on September 28, 2018, then again on January 10, 2019. After the government refused to do so, the defense moved on February 12, 2019, then again on March 11, 2019 for the Court to compel the government to produce this evidence. The defense then moved pursuant to CIPA Section 4 for access to the forensic crime scene in June 2019.

2. The government lies to the Court in its *ex parte* CIPA 4 motion

In accordance with CIPA, the government filed an *ex parte* CIPA 4 motion regarding classified information it does not want to disclose to the defense. In this motion, which the defense obviously never saw, the government **lied** to this Court about the significance and relevance of DevLAN forensic materials. In the Court's Order dated July 22, 2019 denying the defense's CIPA 4 motion for access to the forensic materials, the Court wrote "[t]he Government states that the only forensic evidence that is consistent with the removal of the leaked information is on the Schulte Work station, and uses this conclusion to justify turning over only some data from Schulte's Workstation—the data that supports the Government's theory of its case." *Id.* At 10. As the Court saw at trial, this is clearly false. The government advocated a very convoluted and complex theory at trial involving not only the Schulte Workstation but also the ESXi and FS01 server. The government argued that I used the CIA Workstation to gain unauthorized access to the ESXi server to gain unauthorized access to the Confluence Virtual Machine to access Atlassian backups from the FS01 server. The government lied to this Court.

United States v. Schulte, S3 17 Cr. 548 (PAC); September 14, 2021 letter from *pro se* defendant

3. Motion for reconsideration

The defense then moved again for access to the forensic crime scene on July 18, 2019, August 26, 2019, October 15, 2019, October 28, 2019, November 15, 2019, and December 3, 2019. The Court never ruled on these outstanding motions.

4. Mistrial

The defense moved for a mistrial when the government presented its complex forensic case involving not only the Schulte Workstation, but also the ESXi and FS01 servers, and the fact that these forensic images were provided to the government's own experts; these experts characterized the forensic images as critical to their analysis and opinion—from which they could not have found the forensic artifacts in unallocated space or constructed their timeline and theory of prosecution. The defense moved for a mistrial due to the government's failure to produce these same forensic images to the defense. See Dkt. 328, 331.

5. Defense unable to challenge government's experts or theory of prosecution

The defense then wrote to the Court on February 26, 2020, Dkt. 335:

We write to advise the Court, as we have already advised the government, that the defense is unable to call its computer expert, Dr. Steven M. Bellovin, as a trial witness. As we have previously explained, Dr. Bellovin, despite repeated requests, was never permitted access to the full "mirror images" of the CIA's ESXi and FS01 Servers—images to which the government's expert has long been granted full and unrestricted access.

The fundamental unfairness of a one-sided trial where the defendant is deprived of the ability to present any defense at all clearly compels this Court to action. I already went to trial without the evidence to mount a proper defense in contravention of clearly established law. In England during the 1500s, common law dictated those accused of treason were forbidden counsel and not permitted to call witnesses. The government appears to have resurrected this 16th century common law in lieu of the Constitution, and convened a trial in which I could not rebut the government's witnesses, could not verify their test results, could not properly cross-examine them, could not conduct independent analysis, and could not subject the government's case to adversarial testing. Instead, the government used CIPA improperly, as a shield to prevent legitimate discovery, which it wielded to stage a faux "trial" and manifest injustice.

B. Significance of forensic crime scene

The defense has repeatedly beat this dead horse. But, for a brief summary of the most important issues, the significance of the forensic crime scene is recounted here. At trial, multiple government witnessed testified to the relevance and significance of not only the Schulte workstation but also the ESXi and FS01 servers.

1. The government's case-in-chief

Patrick Leedom, on direct examination (Tr. 926-28) (bold emphasis added):

Q. Now, as part of your responsibilities and participation in this investigation, did you examine forensic files and data from the DevLAN network?

A. Yes, I did.

Q. Did that include reviewing ***the computer the defendant used to access DevLAN*** *while working at the CIA?*

A. Yes, it did.

Q. Did it also include ***reviewing servers connected to DevLAN****?*

A. Yes, it did.

Q. Approximately how much time have you spent over the past two and a half-plus years reviewing those materials?

A. Countless hours.

Q. Have you formed an opinion as to some of the defendant's activities on the DevLAN network in April of 2016?

A. Yes, I have.

Q. I want to focus your attention on April 20, 2016. Have you reached an opinion as to the defendant's activities on the DevLAN network that day?

A. Yes, I have.

Q. What are some of the opinions that you've reached about the defendant's activities on April 20, 2016?

A. On April 20, 2016, the defendant accessed the Confluence virtual machine, which was running on the OSB ***ESXi server****. He then reverted that virtual machine to the 4/16 backup that you've heard about ISB having had made before they changed the passwords. That backup gave him access to the machine again after the passwords were changed. During that time the machine stayed in a reverted state for a little over an hour, and the defendant copied the Confluence backups from the* ***Altabackup server****.*

Also during that time, the defendant deleted many log files both on the ***ESXi server*** *itself and on the virtual machine by reverting to the previous snapshot and deleting it.*

There can be no question that the CIA Workstation, the ESXi server, and the FS01 (Altabackup) server constitute the alleged crime scene in this case and the crux of the government's case-in-chief. Accordingly, Fed. R. Crim. P. 16(a)(1)(E)(ii) clearly establishes that the government must produce forensic images of these three servers to the defense.

As stated in *United States v. Kattar*, 840 F.2d 118, 127 (1st Cir. 1988), a "criminal trial should be viewed not as an adversarial sporting contest, but as a quest for truth." Thus the investigative machinery of the government should be available to seek the truth, not merely to convict, inasmuch as an erroneous conviction would not serve the purposes of law enforcement or justice.

2. Timing analysis critical to identifying which backup was stolen from the CIA

The government sought to prove at trial that the data released by WikiLeaks derived from a specific backup file. To prove this, the government relied upon the complete forensic image of the FS01 (Altabackup) server—it compared the data on WikiLeaks with *each and every one of the backups* on the FS01 server until it found the closest match. The government's second forensic expert, Michael Berger, testified to this "Timing analysis." (Tr. 1351-52):

Q. Were you asked to conduct any analysis of the EDG information disclosed by WikiLeaks?

A. Yes, I was.

Q. Have you formed any opinions with respect to that information?
A. Yes, I have.

Q. What opinions have you formed?
A. I was asked to perform analysis and conduct a timing analysis and look at the data that was on WikiLeaks. My opinion of that analysis is that the data that was released on WikiLeaks came from a date range between March 2 and March 3, 2016.

Q. Was there a backup in existence on the Confluence – was there a Confluence backup file in existence on DevLAN within that time range?
A. Yes.

Q. Which one was that?
A. It was the March 3 backup.

Q. So, if we go to the next slide and move on to the next one after that. I'd like to start with how you arrived at that opinion. Could you describe your methodology, please?
A. Sure. So, I was asked to look at the data that was on WikiLeaks and determine when it came from in the Confluence system. In order to do that, we looked at the concept of version control, which both Stash and Confluence employ. Version control is a basic ability where you can make up dates to documents or source code. And when you save them, they don't completely overwrite your previous versions. The system keeps track of the history of versions so it goes from version 1, version 2.

[...]

Q. I'm sorry to interrupt.
A. That's okay. Because we knew that the version control existed on those systems, we could look at activity that happened on those systems and we could look at data that was posted on WikiLeaks. We then looked for examples of data points of data that was saved in the system that was present on WikiLeaks. And data that was saved in the system that was not present on WikiLeaks.

The government's forensic expert, Michael Berger, utilized his unfettered access to the full forensic images to conduct a timing analysis. Berger's analysis could not be cross-examined, verified, or challenged because the defense did not have access to the forensic images, and therefore could not reproduce Berger's timing analysis. Since the government's case depends upon Berger identifying one specific backup file as the originating data, if the defense were given access to the backups and a forensic expert could rebut the government's expert and identify any other backup file as the originating data, then I must be acquitted. However, as occurred throughout trial, the government relied on the full forensic images to effectively prosecute the case while the defense could not rebut anything through independent analysis or adversarial testing.

3. The Supreme Court clearly established that the Due Process Clause of the Fifth Amendment compels the government to provide equal access to private experts retained by the defense just as it does for its own experts

The Supreme Court noted in *Wardius v. Oregon*, 412 US 470 (1973), that "[a]lthough the Due Process Clause has little to say regarding the amount of discovery which the parties must be afforded, ...it does speak to the *balance of forces* between the accused and his accuser." (emphasis added). Accordingly, "*Wardius* holds that rules about pretrial discovery in criminal prosecutions must apply to prosecutors as well as to defendants. **Access provided to private experts retained by the prosecution must be provided to private experts retained by the defense.**" *United States v. Shrake*, 515 F.3d 743 (7th Cir. 2008) (emphasis added); "Fundamental fairness is violated when a criminal defendant on trial for his liberty is denied the opportunity to have an expert of his choosing, bound by appropriate safeguards imposed by the Court, examine a piece of critical evidence whose nature is subject to varying expert opinion." *Barnard v. Henderson*, 514 F.2d 744, 746 (5th Cir. 1975).

The government's forensic expert, Patrick Leedom, was granted unfettered access to the alleged forensic crime scene, and in fact, all of DevLAN, to conduct his forensic examinations and investigation (Tr. 1148) (bold emphasis added):

Q. And when you worked in their lab, did they give you ***full access*** *to what is a* ***full image*** *of the* ***FSO1 server****?*

A. Yes.

Q. And they gave you, did they not, access to the ***full image of the Atlassian server****, correct?*

A. That's correct.

Q. They gave you ***full access****, did they not, to* ***Mr. Schulte's workstation****, correct?*

A. Correct.

1159-60:

Q. Let me make it easy for you. You tell me what you were given.

A. Sure. ***We were given images of all of the DevLAN machines*** *-- computers, servers -- that were available at the time that we showed up to analyze.*

Q. ***All of them, correct****?*

A. ***Yes.***

Q. Now, you testified that you were also given access to the Atlassian server, right?

A. Uh, yes.

Q. And is it fair to say that the CIA gave you access all throughout the three years you worked with them on this case? Correct?

A. Yes.

1186-87:

Q. Okay. When you examined -- did you by any chance actually physically examine any thumb drives that Mr. Schulte used?

A. ***I had images of those thumb drives.*** *I've seen pictures for them, but I had forensic images of them.*

Q. You had a full forensic image, correct?

A. That's correct.

Q. How many thumb drives did you have a full forensic image of?

A. A lot.

Q. A lot. How many is a lot?

A. Over the network, there were -- dozens.

Q. Right, and you had physical -- I mean, you had access to every one of those mirror images, correct?

A. Yes.

*Q. In fact, you had access to the **mirror images** of **almost every network and every computer that you needed** from the CIA, correct?*

*A. **Yes.***

*Q. **And that very much informed your expert opinion here, correct**?*

*A. **Correct.***

"The ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts. The very integrity of the judicial system and public confidence in the system depend on full disclosure of all the facts, within the framework of the rules of evidence. To ensure that justice is done, it is imperative to the function of the courts that compulsory process be available for the production of evidence needed either by the prosecution or by the defense." *United States v. Nixon*, 418 US 683, 709 (1974).

C. Due to the government's lies and Brady Violations, this Court should compel production of the forensic crime scene

Due to the government's most recent Brady Violation, the Court should order production of not only the improperly concealed AFD and WTF forensic analysis and reports, but also the forensic crime scene as alleged by the government: The Schulte CIA Workstation, the ESXi Server, and the FS01 server.

Respectfully submitted,

Joshua Adam Schulte

Schulte